

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A device-to-device authentication system for authenticating when devices on a network are connected within a certain range, comprising:

a first device comprising:

a first mediating device interface for physically connecting a removable mediating device,

a second device comprising:

a second mediating device interface for physically connecting the removable mediating device,

a network interface unit configured to receive a request for authentication over the network, and

a local environment management unit configured to authenticate that the first device and the second device are connected within the certain range when the first device has physically connected to the removable mediating device within a predetermined period of time before or after the removable mediating device is physically connected to the second device,

wherein the first device can use content when the first device is authenticated.

2. (Previously Presented) The device-to-device authentication system according to claim 1, wherein:

- the second device is a home server,
- the first device is a client for making a request for the content to the home server; and,
- in response to authentication of the client, the home server provides the content and/or issues a license for the content to the client.

3. (Previously Presented) The device-to-device authentication system according to claim 1, wherein:

- two or more home servers are able to be installed on the network; and
- at least one of the home servers provides the content and/or issues a license for the content to a client that is authenticated.

4. (Previously Presented) The device-to-device authentication system according to claim 3, wherein the client is able to be receive provision of the content and/or issuance of the license from at least one of the two or more home servers on the network.

5. (Previously Presented) The device-to-device authentication system according to claim 3, wherein upon connection to a home server on a second network, the client is not able to use the content from the two or more home servers.

6. (Previously Presented) The device-to-device authentication system according to claim 1, wherein the removable mediating device is capable of retaining predetermined identification information for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time.

7. (Previously Presented) The device-to-device authentication system according to claim 1, wherein:

the removable mediating device comprises a memory for retaining confidential information, for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time, in a secure manner.

8. (Previously Presented) The device-to-device authentication system according to claim 7, wherein the confidential information is erased after the predetermined period of time elapses.

9. (Currently Amended) A device-to-device authentication method for authenticating when devices on a network are connected within a certain range, comprising:

physically connecting a removable mediating device to a first physical mediating device interface of a first device;

physically connecting the removable mediating device to a second physical mediating device interface of a second device;
receiving a request for authentication over the network;
authenticating that the first device and the second device are connected within the certain range when the first device physically connected to the mediating device within a predetermined period of time before or after the removable mediating device is physically connected to the second device; and
allowing the first device to use content when the first device is authenticated.

10. (Previously Presented) The device-to-device authentication method according to claim 9, wherein:

the second device is a home server,
the first device is a client for making a request for the content to the home server; and,
in response to authentication of the client, the home server provides the content and/or issues a license for the content to client.

11. (Previously Presented) The device-to-device authentication method according to claim 9, wherein:

two or more home servers are able to be installed on the network; and
at least one of the home servers provides the content and/or issues a license for the content to a client that is authenticated.

12. (Previously Presented) The device-to-device authentication method according to claim 11, wherein the client is able to be receive provision of the content and/or issuance of the license from at least one of the two or more home servers on the network.

13. (Previously Presented) The device-to-device authentication method according to claim 11, wherein upon connection to a home server on a second network, the client is not able to use content from the two or more home servers.

14. (Previously Presented) The device-to-device authentication method according to claim 9, further comprising:

storing predetermined identification information, for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time, in the removable mediating device.

15. (Previously Presented) The device-to-device authentication method according to claim 9, further comprising:

storing confidential information, for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time, in a secure manner in the removable mediating device.

16. (Previously Presented) The device-to-device authentication method according to claim 15, wherein the confidential information is erased the predetermined period of time elapses.

17. (Currently Amended) A communication apparatus for using content on a network within a predetermined allowable range, comprising:

a mediating device interface for physically connecting a removable mediating device;

a network interface for receiving or transmitting a request for authentication over the network; and

a local environment management unit configured to authenticate that the apparatus is within the predetermined allowable range when the apparatus and a device have physically connected to the mediating device within a predetermined period of time between connections, to control the use of the content.

18. (Currently Amended) The communication apparatus according to claim 17, further comprising:

a unit ~~configure~~ configured to receive the content and/or issuing a license for the content when the device and the apparatus are authenticated,

wherein the communication apparatus operates as a home server for providing content on the network;

19. (Currently Amended) The communication apparatus according to claim 17, further comprising:

a unit ~~configure~~ configured to receive provision of the content and/or a license for the content when the device and the apparatus are authenticated, wherein the communication apparatus operates as a client for making a request for the content to a home server on the network.

20. (Previously Presented) The communication apparatus according to claim 19, wherein the unit configured to receive provision of the content and/or issuance of a license for the contents from the two or more home servers authenticated by the local environment management means.

21. (Previously Presented) The communication apparatus according to claim 19, wherein upon connection to a home server on a second network, the client is not able to use the content acquired from the home server on the network.

22. (Previously Presented) The communication apparatus according to claim 17, wherein the removable mediating device is capable of retaining predetermined identification information for determining that the communication apparatus and another device have connected to the removable mediating device within the predetermined period of time.

23. (Previously Presented) The communication apparatus according to claim 17, wherein, the removable mediating device comprises a memory for retaining confidential information, for determining that the communication apparatus and another device have connected to the removable mediating device within the predetermined period of time, in a secure manner.

24. (Previously Presented) The communication apparatus according to claim 23, wherein, the local environment management unit authenticates that the another device, which reads same confidential information from the mediating device and/or reads the confidential information within a predetermined period of time, is located in the local environment of the local environment management means.

25. (Previously Presented) The communication apparatus according to claim 23, wherein the confidential information is erased after a predetermined period of time from generation elapses.

26. (Currently Amended) A computer-readable medium storing a program for causing a computer to execute a method for authenticating whether or not devices on a network are connected within a certain scope, the method comprising:

receiving a request for authentication over the network;

authenticating that a first device and a second device are connected within a certain scope the first device physically connected to a removable mediating device

within a predetermined period of time before or after the removable mediating device physically connected to [[a]] the second device, and

allowing the first device to use content when the first device is authenticated.

27. (Previously Presented) The device-to-device authentication method according to claim 9, further comprising:

writing a temporary random number to the mediating device;
reading the temporary random number from the mediating device; and
collating the temporary random number.